

Spionage-Software Pegasus auf Schweizer iPhones entdeckt

31. Oktober 2018

Sven Millischer, Handelszeitung

Mit Pegasus werden iPhones zur Abhörfalle. Nun gibt es Hinweise, dass die umstrittene Spyware auch in der Schweiz eingesetzt wurde.

Ein Klick genügt, und aus dem eigenen iPhone wird ein veritables Abhörinstrument. Die Falle, ein sogenannter «exploit link», kommt zumeist in Form einer unverfänglichen Whatsapp-Nachricht, einer E-Mail oder SMS daher. Sobald der Nutzer auf den Link klickt, installiert sich Pegasus, etabliert eine Server-Verbindung.

Fortan saugt die Spyware sämtliche iPhone-Daten ab und schickt sie unbemerkt vom User an den jeweiligen Operator: Von den Standortdaten über den Browserverlauf bis hin zu Mikrofonaufnahmen, Kontaktdaten oder Telefon-Gesprächen. Das eigene Smartphone wird zum offenen Buch für Schnüffler.

Was nach Orwell in der Hosentasche tönt, wird möglicherweise auch in der Schweiz praktiziert. So hat das «Citizen Lab» der Universität Toronto vor einigen Wochen eine Untersuchung zur Spyware der israelischen Sicherheitsfirma NSO Group veröffentlicht. Den Forschern ist es gelungen, Daten-Spuren («DNS Cache Probing») von Pegasus in 45 Ländern nachzuweisen. Darunter befindet sich auch die Schweiz als eines von wenigen Länder Westeuropas.

Mit anderen Worten: Eine unbekannte Organisation hat die israelische Schnüffelssoftware möglicherweise auch hierzulande im Einsatz gehabt. Die «Citizen Lab»-Autoren konnten nämlich einen für die Schweiz dedizierten Pegasus-Operator festmachen, den sie auf den Namen «Edelweiss» taufen. Dieser Operator war gemäss kanadischer Studie von Juli 2017 bis zum Untersuchungsschluss im Frühherbst über das Netz der Swisscom aktiv.

Man habe dazu Untersuchungen eingeleitet, sagt Swisscom-Sprecher Armin Schädeli: «Wir konnten keine Anhaltspunkte finden, dass über das Swisscom-Netz mit Pegasus kommuniziert wird.» Man behalte die Situation aber im Auge und reagiere auf allfällig neue Erkenntnisse.

Besondere Informatikprogramme

Bill Marczak, Co-Autor der Pegasus-Studie, geht davon aus, dass die von ihm festgestellte Nutzung in der Schweiz legal ist: «Da NSO Group die Software ausschliesslich an Staaten verkauft, könnte Pegasus beispielsweise bei Strafverfolgern oder Geheimdiensten im Einsatz sein.»

Millionengeschäft mit Spyware

Die israelische Firma NSO Group entwickelt Überwachungssoftware für Staaten. Deren Pegasus-Software soll in der Lage sein, Smartphone zu hacken und die gesamten Medien und Inhalte weiterzuleiten.

NSO betont, dass die Spyware nur im Kampf der Strafverfolger gegen Kriminalität und Terrorismus eingesetzt werde. Allerdings gibt es zahlreiche Berichte und Studien, die darauf hindeuten, dass Abnehmer-Staaten wie Saudi Arabien oder Mexiko die NSO-Tools auch gegen Dissidenten und Journalisten einsetzen.

Gemäss einem Artikel der «New York Times» von 2016 kostet es rund 1,2 Millionen Dollar, um mit Pegasus zehn Besitzer eines iPhones auszuspionieren, davon kostet die Installation eine halbe Million Dollar.

Das Bundesamt für Polizei Fedpol gibt sich allerdings zugeknöpft. «Aufgrund der vertraglich geregelten Vertraulichkeit, geben wir keine Informationen über unsere Partner Preis, weder über Partner, mit denen wir zusammenarbeiten noch über Partner, mit denen wir nicht zusammenarbeiten», sagt Fedpol-Sprecher Thomas Dayer und verweist auf die Behörde «Überwachung Post- und Fernmeldeverkehr». Dieser wird im nächsten Jahr erstmals Statistiken veröffentlichen zur Anwendung von «besonderen Informatikprogrammen durch die Strafverfolgungsbehörden».

Es geht dabei um «GovWare» wie beispielsweise Pegasus. Sie kann als Zwangsmassnahme bei schweren Straftaten eingesetzt werden. Seit einem Jahr hat auch der Nachrichtendienst des Bundes die Möglichkeit, elektronische Überwachungsmassnahmen anzuordnen.

Politisch motivierte Attacken

Es bleibt jedoch offen, ob hiesige Strafverfolger oder Geheimdienstler die genannte Spysoftware im Einsatz haben. Sollte dem so sein, wäre deren Beschaffung zumindest fragwürdig. Denn die «Citizen Lab»-Autoren legen ebenfalls dar, dass die NSO Group ihre Pegasus-Software an Länder liefert wie Bahrain, Kazachstan, Mexiko oder Saudi Arabien liefern.

Länder, in denen die Spyware nicht nur im Rahmen der Strafverfolgung zum Einsatz kommt, sondern offenbar auch gezielt gegen Mitglieder der Zivilgesellschaft eingesetzt wird. Ob mexikanische Journalisten oder saudische Dissidenten, sie alle wurden gemäss «Citizen Lab» zur Zielscheibe von politisch motivierten Schnüffelattacken qua Pegasus.

Nach Veröffentlichung der Studie liess die betroffene Firma, NSO Group, ein Statement verbreiten: Man stelle Produkte mit dem einzigen Zweck her, «Verbrechen und Terror zu verhindern und aufzuklären». Die «Citizen Lab»-Untersuchung weise zahlreiche Fehler auf. So operiere NSO in vielen der aufgeführten Länder gar nicht. Zudem habe man ein strenges «Business Ethics Framework», das eine Zusammenarbeit mit Partnerländern vorgängig genau prüfe. Sollte es Verdacht auf Missbrauch geben, gehe man dem nach.

Da «Citizen Lab» den Schweizer Pegasus-Operator bereits im Juli 2017 entdeckt hat, stellt sich die Frage, wer den Staatstrojaner überhaupt hätte legal einsetzen sollten. Das neue Nachrichtendienstgesetz gilt seit September 2017, das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs gar erst diesem Frühjahr März. Ein privater IT-Forensiker tippt auf den israelischen Geheimdienst, der «zahlreiche Aktivitäten zur Überwachung von Schweizer Zielen» hat. Es bleibt eine Mutmassung.